ABSTRACT OF THE DISCLOSURE

A system, method, and computer readable medium for the proactive detection of malware in operating systems that receive application programming interface (API) calls is provided. A virtual operating environment for simulating the execution of programs and determining if the programs are malware is created. The virtual operating environment confines potential malware so that the systems of the host operating environment will not be adversely effected. During simulation, a behavior signature is generated based on the API calls issued by potential malware. The behavior signature is suitable for analysis to determine whether the simulated executable is malware.